DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, DC 20380-0001

MCO 3093.2
CSA
11 Jan 93

MARINE CORPS ORDER 3093.2

From: Commandant of the Marine Corps
To: Distribution List

Subj: U.S. MARINE CORPS POLICY FOR THE IMPLEMENTATION AND MANAGEMENT OF THE GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE (GOSIP)

Ref: (a) Assistant Secretary of Defense Memorandum, DoD Policy on the GOSIP Data Communications Protocols, September 25, 1990 (NOTAL)
(b) U.S. Marine Corps (USMC) Government Open Systems Interconnection Profile (GOSIP) Transition and Management Plan

Encl: (1) GOSIP Waiver Procedures
(2) GOSIP Waiver Chain of Authority
(3) Acronyms and Abbreviations
(4) Definitions

1. Purpose. This Order implements the Department of Defense (DoD) policy on the Government Open Systems Interconnection Profile (GOSIP). It establishes policy, management goals, and procedures necessary to migrate to a GOSIP-compliant open systems operating environment. It also ensures that interoperability in existing information systems will be maintained throughout the transition to a GOSIP operating environment.

2. Background. The Assistant Secretary of Defense, Command and Control, Communications and Intelligence (ASD (C3I)) established DoD's commitment to using GOSIP standards by mandating their use, including tactical systems in reference (a).

a. Applicability. The policies contained in this Order apply to major upgrades of all Marine Corps information systems, data communications systems, and networks as well as the development, procurement, production, and maintenance of new systems. Systems provided to the Marine Corps but managed by another service must be reviewed on a case by case basis to determine whether Marine Corps or other GOSIP policy applies. Similarly, Marine Corps GOSIP implementation plans must be reviewed with other service/agency GOSIP implementations to ensure interoperability. Enclosure (1) provides decision criteria to be used in evaluating GOSIP applicability to a system. Enclosure (2) provides the GOSIP waiver chain of authority. Definitions of acronyms, abbreviations, and terms are included in enclosures (3) and (4).

b. Description

(1) Automated information systems (AIS's) are utilized throughout the Marine Corps in the Supporting Establishment (SE) and operating forces both tactically and nontactically. Protocol standards delineate the sets of rules or conventions governing the exchange of information between computer systems, which also includes their peripheral devices. They can be either technical or procedural standards. The same protocol standards must be used between systems to establish interoperability.

(2) GOSIP is a protocol standards suite subset of the International Standards Organization Open Systems Interconnection protocol standards suite. GOSIP is also part of the ongoing DoD standardization efforts within the Open Systems Environment (OSE).

(3) OSE provides the comprehensive set of interfaces, services, and supporting formats for interoperability of applications. OSE consists of the Information Transfer component (of which GOSIP is a part), Information component, and Information Processing component. OSE uses Corporate Information Management's (CIM's) Technical Reference Model to specify the appropriate standards within each OSE component. OSE provides end-to-end interworking among end users. GOSIP provides an intercomputer connection function by unifying the information transfer portion of OSE.

c. Data Communications Standards. The Data Communications Protocol Standardization (DCPS) program offers the forum which develops and enhances standards for military requirements. The Defense Information Systems Agency (DISA) is responsible for these standards. The Military Communication-Electronics Board (MCEB) affords a means to provide DoD interests in the international standards bodies. The Information Technology Policy Board as part of the Corporate Information Management office establishes standards for business applications.

d. GOSIP Evolution. The mandatory use of GOSIP standards is applicable as the GOSIP protocols become suitable for satisfying a system's functionality. GOSIP Version 1.0 protocol suite became mandatory after August 15, 1990 when published as Federal Information Processing Standard (FIPS) Publication Number 146. The phased implementation of subsequent GOSIP versions will incorporate international standards and will eventually incorporate the full functionality of the GOSIP protocol suite. GOSIP versions will be updated periodically, usually annually.

e. GOSIP Benefits. DoD components must develop individual GOSIP Interoperability and Transition Plans which provides a coordinated transition to GOSIP protocols without disrupting the services provided by current data systems. Some fundamental reasons for implementing GOSIP protocols are:

(1) Greater interoperability among diverse users/Services/agencies.

(2) Cost savings associated with sharing similar technology.

(3) Increased effectiveness through efficient use of information resources.

f. Discussion. The fundamental goal of this Order is to provide guidance and management policy for the use of GOSIP standards. The orderly transformation of current protocol suites to GOSIP-compliant protocol suites must maintain reliable and responsive systems in support of the Marine Corps missions. Anticipated extensive cost and scope will greatly affect GOSIP implementation. Translation devices or gateways, and other internetworking tools such as routers and bridges will be required during a period of coexistence with existing standards to assure interoperability.

3. Execution

a. Transition to GOSIP. All Marine Corps AIS's and networks will eventually be GOSIP compliant, as GOSIP evolves to satisfy the military requirements. Translation devices or gateways, routers/bridges may be used for those systems existing before GOSIP became mandatory and for accommodating military issues not incorporated into GOSIP. The use of such devices shall be limited to the coexistence period and not used as a preferred solution for GOSIP implementation.

b. Marine Corps Registration Authority. The Assistant Chief of Staff, Command, Control, Communications, Computer, and Intelligence (AC/S C4I) is the senior Marine Corps GOSIP Registration Authority. The Marine Corps Computer and Telecommunications Activity (MCCTA) is the organization within C4I which is responsible for the execution of Marine Corps Registration Authority duties. All requests for registering Network Service Access Point (NSAP), Session Service Access Point (SSAP), Transport Service Access Point (TSAP), Originator/Recipient (O/R) addresses, Object Identifiers (OID), and X.500 Directory names shall be forwarded to MCCTA.

c. Acquisition Consideration. Acquisition considerations dictate that, where possible, a commercial-off-the-shelf (COTS) solution must be used when it meets the needs for a program. However, COTS products will be procured until after they have been certified as GOSIP compliant. The National Institute of Standards and Technology (NIST) maintains a list of approved GOSIP products called the Register of Conformance Tested GOSIP Products. MCCTA will assist Marine Corps organizations to obtain copies of this list.

d. GOSIP Waivers. GOSIP applicability will be waived for specific time periods where it can be clearly demonstrated that there are significant performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the waiver. Waivers shall be requested when functionality critical to the Marine Corps mission is not included in GOSIP-compliant products. DCPS program enhanced GOSIP standards do not require a waiver insomuch that the lack of GOSIP functionality is accommodated by the enhancement. This enhancement renders the standard as an equivalent to the GOSIP standard. Waivers shall be requested for special purpose networks which will not be required to interoperate with other networks. However, only in rare circumstances will such waivers be granted, inasmuch as future scenarios and joint operations may necessitate interoperability not envisioned earlier. Waivers to the GOSIP policies because of GOSIP inadequacies must consider future versions of GOSIP for the added functionality which may be incorporated at a future date. Information systems developers must be prepared to reevaluate the adequacy of GOSIP once new functionality is introduced into GOSIP. A waiver can be requested at any point in the life cycle of a system and at any relevant point in the procurement cycle. The following general decision criteria shall be used to determine whether information systems require a GOSIP waiver (see enclosure (1)).

(1) The system will be isolated without a potential need for information exchange with other information systems.

(2) The functionality contained in GOSIP does not satisfy the operational requirements of the system.

(3) The system considered is neither a new information system nor a major upgrade. A major upgrade is a subjective term, and is defined in enclosure (4). Briefly, an upgrade will be considered to be major when a critical component is replaced or modified. A critical component for GOSIP compliance is defined to mean hardware or suites of software that affect the interoperability and internetworking abilities of the system. For example, when the Front End Processor (FEP) to a mainframe computer is upgraded, the critical nature of this component for networking makes this a major upgrade.

e. Marine Corps GOSIP Waiver Approval Authority. AC/S C4I is the senior Marine Corps GOSIP waiver approval authority. All Marine Corps GOSIP waiver requests receive final approval from Assistant Secretary of the Navy, Research, Development, and Acquisition ASN (RD&A) via Deputy Assistant Secretary of the Navy, Command, Control, Computer, Communications, Intelligence, Space, and Electronic Warfare (DASN (C4I/SPACE/EW)). Enclosure (2) shows the GOSIP waiver chain of authority.

f. GOSIP Working Group. A GOSIP Working Group will meet as necessary to resolve any GOSIP related policy and implementation issues that affect the Marine Corps. The GOSIP Working Group will be chaired by AC/S C4I and will consist of representatives from HQMC, MCCDC, MARCORSYSCOM, and MCCTA. Participation by system/functional sponsors on issues applicable to them will be occasionally required. The purpose of this working group is to provide an effective forum for coordinating Marine Corps development efforts within Department of the Navy (DON) and DoD policies. Where agreement cannot be reached, issues will be raised to the ISSC.

4. Responsibilities. The following organizational functions describe the responsibilities for including GOSIP standards in Marine Corps information systems planning, development, and procurement actions:

a. Commandant of the Marine Corps (CMC). CMC, through AC/S C4I establishes Marine Corps GOSIP policy. Marine Corps policy requires compliance with DoD policy and with joint/combined policy as directed by DoD.

b. Counsel for the Commandant CMC(CL). CMC(CL) is responsible for advice concerning the legal sufficiency of actions related to Automatic Data Processing (ADP) procurement. CMC(CL) is consulted with respect to the legal sufficiency of a request for GOSIP waiver. A significant number of statutes and regulations apply to ADP procurement, including procurement subject to GOSIP or a waiver thereof.

c. Executive Steering Group (ESG). The ESG is the highest level planning, programming, and budgeting forum within the Marine Corps. It determines the Marine Corps programs, including alternatives, to be submitted to CMC for approval. The ESG addresses issues, presented by the Chairman of the Information Systems Steering Committee, dealing with information systems and supporting information resources.

d. Information Systems Steering Committee (ISSC). The ISSC is the designated arm of the CMC Committee that oversees Information Resources Management (IRM)-related issues. The ISSC consists of a general officer grade representative of each member of the ESG, AC/S C4I, and the Director of Administration and Resource Management (AR) Division, Headquarters, U.S. Marine Corps. The ISSC is chaired by the Director, MCCTA. The ISSC coordinates the application and use of tactical and nontactical information systems consistent with overall Marine Corps missions. This committee provides the forum for resolving GOSIP-related policy and implementation issues by addressing them to the AC/S C4I for appropriate action.

e. Assistant Chief of Staff, Command, Control, Communications, Computer, and Intelligence (AC/S C4I). The AC/S C4I is the senior Marine Corps IRM representative and provides for the planning, directing, budgeting, and coordinating of staff activities relating to command and control systems, telecommunications, and AIS's. Waivers to GOSIP compliance for AIS's must be approved by AC/S C4I. GOSIP waiver procedures must be followed in accordance with this Order and reference (b). The Deputy Assistant Chief of Staff, C4I, Systems Integration (DAC/S C4I (CS)) is responsible for the planning and network administration of the Marine Corps Data Network (MCDN). DAC/S C4I (CS) is also responsible for the interoperability of nontactical and tactical information systems.

f. Director, Marine Corps Computer and Telecommunications Activity (MCCTA). MCCTA is responsible to the AC/S C4I for Marine Corps GOSIP compliance records for nontactical systems registration. MCCTA is responsible for determining the adequacy of GOSIP functionality to planned or developing nontactical AIS's and information transfer systems and networks. If existing GOSIP standards are inadequate, MCCTA will request a GOSIP waiver, in accordance with this Order and reference (b). MCCTA is responsible for the technical administration of the MCDN.

g. Commanding General, Marine Corps Combat Development Command (CG MCCDC). CG MCCDC is responsible for identifying and validating FMF information systems and tactical data communications and internetworking requirements.

h. Commander, Marine Corps Systems Command (COMMARCORSYSCOM). COMMARCORSYSCOM is responsible for acquisition of FMF Table of Equipment (T/E) AIS equipment, the configuration management and interoperability testing (MCO 3093.1) of that equipment, and for the development of FMF-specific systems. COMMARCORSYSCOM is responsible for determining the adequacy of GOSIP functionality to planned or developing FMF tactical information systems and information transfer systems and networks. If existing GOSIP standards are inadequate, COMMARCORSYSCOM will request a GOSIP waiver, in accordance with this Order and reference (b). COMMARCORSYSCOM is responsible to the AC/S C4I for Marine Corps GOSIP compliance records for tactical systems registration.

5. Action. The following responsibilities apply to the Marine Corps organizations listed.

a. Assistant Chief of Staff, Command, Control, Communications Computer, and Intelligence (AC/S C4I). AC/S C4I will:

(1) Act, for the Commandant, on all matters pertaining to GOSIP policy.

(2) Represent the Marine Corps on Joint Chiefs of Staff (JCS), DoD, and DON directed GOSIP policy interoperability standards boards and groups.

(3) Establish policies and procedures for implementing GOSIP and insuring GOSIP interoperability.

(4) Provide guidance to CG MCCDC and COMMARCORSYSCOM on GOSIP policy issues considered at policy level meetings.

(5) Act as the Marine Corps Registration Authority and provide centralized management of Marine Corps NSAP, SSAP, TSAP addresses, O/R, OID, and X.500 directory names.

(6) Provide Marine Corps approval of GOSIP waivers for military department approval by Assistant Secretary of the Navy, Research, Development, and Acquisition (ASN(RD&A)). This includes coordination of all GOSIP compliance.

(7) Establish, and provide a chairman for the GOSIP Working Group to resolve GOSIP-related policy and implementation issues. This working group shall make recommendations to the ISSC on all matters pertaining to GOSIP issues.

b. Director, Marine Corps Computer and Telecommunications Activity (MCCTA). MCCTA will:

(1) Support and make recommendations to AC/S C4I on GOSIP policy issues for joint GOSIP policy interoperability standards boards and groups.

(2) As directed by AC/S C4I defend Marine Corps nontactical requirements (especially with GOSIP implementations) with Navy Information Systems Management Command (NISMC).

(3) Provide technical direction on GOSIP to Marine Corps IRM activities.

(4) Review GOSIP waiver requests for Supporting Establishment systems and recommend approval/disapproval to AC/S C4I.

(5) Ensure that requirements documents relating to unique Marine Corps requirements contain a statement, with justification, that the system will never be connected to a network or another AIS, and GOSIP standards are inadequate to provide the functionality required by the system.

(6) Ensure that GOSIP specifications are included in configuration management of information systems.

(7) Coordinate AIS development with CG MCCDC and COMMARCORSYSCOM, as appropriate.

(8) Provide a member to the GOSIP Working Group.

(9) Act as the Marine Corps Registration Authority and provide centralized management of Marine Corps NSAP, SSAP, TSAP addresses, O/R, OID, and X.500 directory names.

(10) Act as the Marine Corps Administrative Authority (AA) for GOSIP records. Ensure that the Marine Corps users are registered with the GOSIP Registration Authority for all GOSIP addresses and objects as the Marine Corps AA. Keep records of GOSIP compliance for all Marine Corps information systems and networks (including communications systems).

(11) In coordination with the Joint Interoperability Test Center (JITC) and NIST, provide technical support to AC/S C4I in certifying that COTS GOSIP products are acceptable for Marine Corps use.

c. Functional Managers (FM) for Nontactical Information Systems Data Communications Systems and Networks under Development. FM's for information systems under development shall:

(1) In coordination with AC/S C4I include GOSIP specifications in requirements documents incorporating applicable GOSIP specifications. Enclosure (1) provides decision criteria for GOSIP specifications, and enclosure (2) provides the GOSIP waiver chain of authority.

(2) In coordination with the JITC, Ft Huachuca, AZ and NIST schedule GOSIP certification testing of COTS GOSIP products with MCCTA, COMMARCORSYSCOM, or AC/S C4I as appropriate.

d. Commanding General, Marine Corps Combat Development Command (CG MCCDC). CG MCCDC will:

(1) Develop operational automated information systems and data communications requirements that consider GOSIP protocols. Ensure that GOSIP waiver documents relating to unique Marine Corps requirements contain a statement, with justification, that the system will never be connected to a network or another AIS, and GOSIP standards are inadequate to provide the functionality required by the system.

(2) Include GOSIP specifications in requirements documents (such as Operational Requirements Document (ORD)) incorporating applicable GOSIP specifications. Enclosure (1) provides decision criteria for GOSIP specifications, and enclosure (2) provides the GOSIP waiver chain of authority.

(3) Ensure that Mission Need Statements (MNS's) and ORD's relating to unique Marine Corps requirements contain a GOSIP waiver statement.

(4) Provide a member to the GOSIP Working Group.

(5) Verify that GOSIP protocols satisfy operational requirements for tactical systems. Recommend modifications to GOSIP standards where they do not fulfill Marine Corps requirements.

(6) In coordination with the appropriate functional managers, specify GOSIP requirements for tactical systems.

e. Commander, Marine Corps Systems Command (COMMARCORSYSCOM). COMMARCORSYSCOM will:

(1) Verify that GOSIP specifications adequately satisfy technical and operational tactical information systems requirements. Recommend modifications to GOSIP standards where they do not adequately fulfill Marine Corps requirements.

(2) Ensure that tactical GOSIP requirements are included in related program, budget, and funding documents.

(3) Ensure that GOSIP requirements are implemented in tactical systems under development unless waived in accordance with this Order. GOSIP waiver documents must contain a statement, with justification, that the system will never be connected to a network or another AIS, and GOSIP standards are inadequate to provide the functionality required by the systems.

(4) Ensure GOSIP issues are thoroughly considered during configuration management of tactical AIS's.

(5) As directed by AC/S C4I, coordinate tactical systems requirements (especially with GOSIP implementations) with DASN (C4I/SPACE/EW).

(6) Provide recommendations on GOSIP waivers for tactical systems to AC/S C4I for final military department approval by ASN(RD&A).

(7) Ensure that the Marine Tactical Systems (MTS) Technical Interface Design Plan (TIDP) reflects GOSIP requirements for networking interfaces.

(8) Provide funding to satisfy GOSIP requirements for tactical systems and networks.

(9) Assist AC/S C4I in representing the Marine Corps on joint GOSIP technical interoperability standards boards and groups for tactical systems.

(10) Assist AC/S C4I in representing the Marine Corps on standards boards and groups to introduce GOSIP enhancements to fulfill Marine Corps operational requirements into the DCPS program.

(11) Provide a member to the GOSIP Working Group.

f. Program Managers (PM's) for Tactical Information Systems, Data Communications Systems, and Networks under Development. PM's for information systems under development shall:

(1) Assist CG MCCDC Proponency and Requirements officers in identifying GOSIP specifications required for MNS's and ORD's.

(2) Ensure that GOSIP specifications are included in configuration management of information systems.

(3) In coordination with the JITC, Ft Huachuca, AZ and NIST schedule GOSIP certification testing of COTS GOSIP products with MCCTA, COMMARCORSYSCOM, or AC/S C4I as appropriate.

6. Records Retention

a. COMMARCORSYSCOM and MCCTA. Maintain GOSIP records as described in the Order. Permanently transfer records to Washington National Records Center when 4 years old. Offer records to National Archives Record Administration when 25 years old.

b. FMF. Retain GOSIP records on board. Destroy records when no longer needed for reference.

7. Reserve Applicability. This Order is applicable to the Marine Corps Reserve.

W. E. BOOMER
Assistant Commandant
of the Marine Corps

DISTRIBUTION: PCN 10203119800

Copy to: 7000110 (55)
8145005 (2)
7000099, 144/8145001 (1)

GOSIP Waiver Procedures

1. General. A waiver from using GOSIP-compliant products will be considered only in exceptional cases as opposed to normal practice. The primary condition that must be met to obtain a waiver is that GOSIP-compliant products are inadequate. The waiver process results in a decision to bypass GOSIP until GOSIP products can satisfy requirements. Use of non-compliant GOSIP systems will be permitted for a period of time that is normally specified in the service/agency transition plan to GOSIP without resorting to waivers. This plan is required from all Federal Government users and permits organizations to phase their transition to GOSIP without disrupting ongoing services. The major intent of GOSIP is to address future procurement while not interfering with the established base. In all cases, consideration should be given to increased costs involved in upgrading or retrofitting GOSIP capabilities, compared to including them initially (up front). Waivers from GOSIP must be published in the Federal Register and other public documents. Therefore, waiver approval must be obtained at the Service Secretary level. All documents obtained during this process become a part of the permanent record for the system.

2. Discussion. When GOSIP protocols do not adequately fulfill requirements, functional managers (FM's)/Program Managers (PM's) must initiate a GOSIP waiver request through the Director, Marine Corps Computer and Telecommunications Activity (MCCTA). The requirements specified in the Request for Proposal (RFP), Mission Need Statement (MNS) or Operational Requirements Document (ORD) must clearly be unsatisfiable by GOSIP protocol standards in order to qualify for a GOSIP waiver. It would be in the best interest of the developer to wait for contractor responses to an RFP before determining GOSIP adequacy. The requirement for a GOSIP waiver applies to all new tactical and nontactical information systems as well as major upgrades to those systems. GOSIP waivers are a temporary deferment from implementing GOSIP protocol standards with a definite expiration date. Waivers will be reevaluated upon expiration to determine if the desired functionality has been added to GOSIP or if the waiver should be renewed. Exclusions from implementing GOSIP protocols will occur only in exceptional cases and will be minimized to reduce life cycle costs later in the system's development.

3. GOSIP Waiver Decision Process. Figure 1-1 shows the GOSIP Waiver Decision Process. The following steps are taken in determining whether a GOSIP waiver is required for a system.

a. Determination of GOSIP Compliance. All of the following steps are to be taken in evaluating a system.

(1) First, information system developers must define the requirements of the information system and determine the adequacy of GOSIP standards.

(2) Second, any system then must be evaluated upon the requirement for internetworking. Information exchange internetworking requires interoperability and use of network resources external to Marine Corps systems (e.g., network directory, data delivery). If so, then it must be GOSIP compliant.

(3) Third, the system must be evaluated to determine whether it is a major upgrade or a new system. If either, then it must be GOSIP-compliant.

(4) Fourth, the requirements of the system must be evaluated against what GOSIP protocols can provide, to determine whether the requirements are satisfied by GOSIP. If so, then it must be GOSIP-compliant.

(5) Lastly, the system must be evaluated against whether there are performance or cost advantages to implementing GOSIP protocols. Detrimental effects which can be offset by DoD-wide savings do not qualify the system for a GOSIP waiver.

b. Developing the Information System. If all of the steps result in positive answers, then a GOSIP-compliant system is developed. After each step is evaluated, if any or all of the steps are negative answers, then the program development enters a process to obtain a GOSIP waiver. The following steps are to be taken in developing such a system.

(1) First, a business case analysis must be developed for systems which justifies the requirement for non-GOSIP compliance.

(2) Second, a GOSIP waiver must then be obtained through the appropriate chain of authority as displayed in figure 1-2.

(3) Third, after receiving the necessary approval, develop the system.

(4) Lastly, the system will be reevaluated, when appropriate, prior to the expiration date of the waiver to reassess the waiver’s basis. This reassessment should determine if GOSIP can meet the requirements of the system, as additional functionality is added to GOSIP and GOSIP protocols evolve. Recommendations to enhance GOSIP standards should be forwarded to the DCPS program standards bodies to gain that functionality in future versions of GOSIP standards.

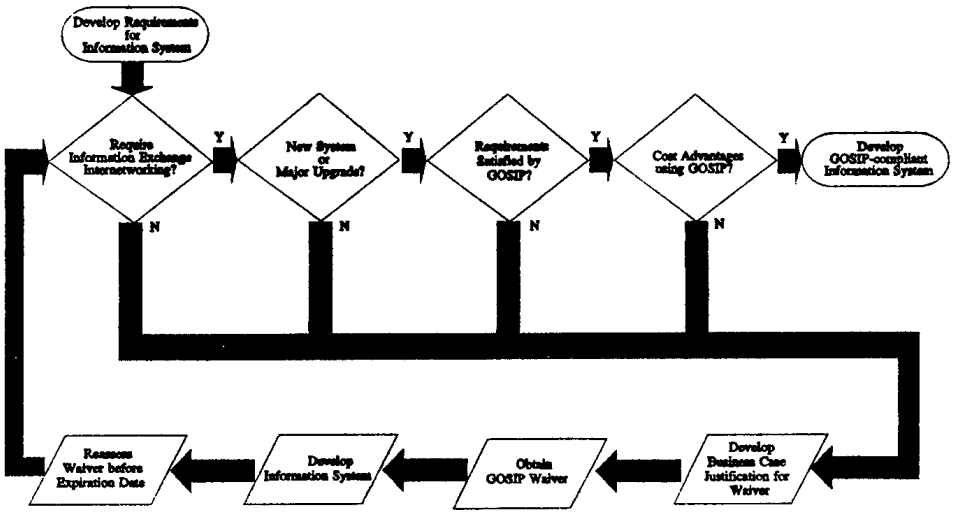

Figure 1-1. GOSIP Waiver Decision Criteria Flowchart

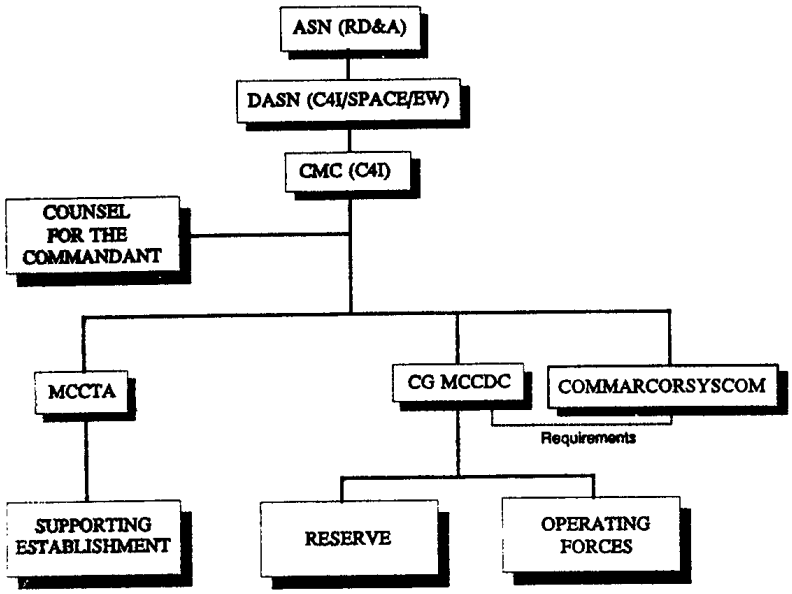

Figure 1-2. GOSIP Waiver Chain of Authority

Acronyms and Abbreviations

AA	ADMINISTRATIVE AUTHORITY
AC/S	ASSISTANT CHIEF OF STAFF
ACMC	ASSISTANT COMMANDANT OF THE MARINE CORPS
ADP	AUTOMATED DATA PROCESSING
AIS	AUTOMATED INFORMATION SYSTEM(S)
AR	ADMINISTRATION AND RESOURCE MANAGEMENT DIVISION, HQMC
ASN(RD&A)	ASSISTANT SECRETARY OF THE NAVY, RESEARCH, DEVELOPMENT AND ACQUISITION
AUTODIN	AUTOMATED DIGITAL NETWORK
BAN	BASE AREA NETWORK
C4I	COMMAND, CONTROL, COMMUNICATIONS, COMPUTER AND INTELLIGENCE DEPARTMENT, HQMC
CG	COMMANDING GENERAL
CIM	CORPORATE INFORMATION MANAGEMENT
CMC	COMMANDANT OF THE MARINE CORPS
COMMARCORSYSCOM	COMMANDER, MARINE CORPS SYSTEMS COMMAND
COTS	COMMERCIAL-OFF-THE-SHELF
CS	SYSTEMS INTEGRATION DIVISION, HQMC
DAC/S C4I(CS)	DEPUTY ASSISTANT CHIEF OF STAFF; COMMAND, CONTROL, COMPUTER, COMMUNICATIONS, AND INTELLIGENCE; SYSTEM INTEGRATION DIVISION, HQMC
DASN(C4I/SPACE/EW)	DEPUTY ASSISTANT SECRETARY OF THE NAVY, COMMAND AND CONTROL, COMPUTERS AND COMMUNICATION, INTELLIGENCE, SPACE AND ELECTRONIC WARFARE
DCPS	DATA COMMUNICATIONS PROTOCOL STANDARDIZATION
DDN	DEFENSE DATA NETWORK
DISA	DEFENSE INFORMATION SYSTEMS AGENCY
DON	DEPARTMENT OF THE NAVY
ES	END SYSTEM
FEP	FRONT END PROCESSOR
FIPS	FEDERAL INFORMATION PROCESSING STANDARD
FM	FUNCTIONAL MANAGER
FMF	FLEET MARINE FORCE
GOSIP	GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE
HQMC	HEADQUARTERS, U.S. MARINE CORPS

IRM	INFORMATION RESOURCES MANAGEMENT
ISSC	INFORMATION SYSTEMS STEERING COMMITTEE, HQMC
JCS	JOINT CHIEFS OF STAFF
MARCORSYSCOM	MARINE CORPS SYSTEMS COMMAND
MCCDC	MARINE CORPS COMBAT DEVELOPMENT COMMAND
MCCTA	MARINE CORPS COMPUTED AND TELECOMMUNICATIONS ACTIVITY
MCDN	MARINE CORPS DATA NETWORK
MNS	MISSION NEED STATEMENT
MTS	MARINE TACTICAL SYSTEM
NISMC	NAVY INFORMATION SYSTEMS MANAGEMENT COMMAND
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NSAP	NETWORK SERVICES ACCESS POINT
OID	OBJECT IDENTIFIER
ORD	OPERATIONAL REQUIREMENTS DOCUMENT
OSE	OPEN SYSTEMS ENVIRONMENT
OSI	OPEN SYSTEMS INTERCONNECTION
O/R	ORIGINATOR/RECIPIENT
PM	PROGRAM MANAGER
RFP	REQUEST FOR PROPOSAL
SECDEF	SECRETARY OF DEFENSE
SECNAV	SECRETARY OF THE NAVY
SNA	(IBM) SYSTEM NETWORK ARCHITECTURE
SSAP	SESSION SERVICE ACCESS POINT
TIDP	TACTICAL INTERFACE DESIGN PLAN
TSAP	TRANSPORT SERVICE ACCESS POINT

Definitions

1. Automated Information System (AIS). A combination of information, computer, and telecommunications resources, and other information technology and personnel resources which collects, records, processes, stores, communicates, retrieves, and displays information (DODD 7920.1 and MCO P5231.1B).

2. Bridge. A device that interconnects two networks which may be effectively identical, but where some physical or logical constraint means that a single larger network cannot be used. For example, a bridge may connect two ethernet LANs where a single ethernet LAN may exceed the length limitation.

3. End System (ES). An ES, or host, is a system that contains the application processes that interact with users and performs functions of all seven layers of the OSI Reference Model. This system is viewed as a terminus; i.e., where data transfers originate or terminate.

4. GOSIP Compliance. A statement, resulting from verification, that an ADP system complies with GOSIP specifications and is suitable for Service use.

5. Information Systems. An interacting assembly of procedures, system processes and methods which includes equipment specifically for the purpose of supporting the command and control of military forces. This equipment is accounted for on both the Table of Allowable Material and local supply accounts. The term specifically includes, but is not limited to:

    a. Command and control systems

    b. Computer systems and equipment

    c. Intelligence systems

    d. Sensor systems and equipment

    e. Communications systems and equipment

6. Interworking. An operating environment which enables access to resources on any system without concern for specific details and limitations. This environment is independent of vendors with wider distribution of services and information available to end users. Its elements resolves differences in data forms, program management and resource management.

7. Internetworking. Communications which require network services and involve host-to-host data interchanges. This type of communications requires a high degree of interoperability to be effective.

8. Interoperability

a. The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together (Joint Pub 1-02).

b. The condition achieved among communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases (Joint Pub 1-02).

9. Major Upgrade. The redesign or substantial addition of hardware, the rewriting of more than half the software, the redesign of the software architecture, or the substantial addition of new software functions.

10. Marine Corps Critical Computer Resources (MCCR). Computer resources required for the conduct of the military mission of the DoD. This definition includes embedded computer resources used in mission critical systems as well as those ADPE or ADP services related to mission critical systems (MCO 5200.23A). MCCR is to be used in procurement context and not to delineate information management responsibilities.

11. Mission-Critical System. Any system that is required for conduct of the military mission of the DoD. This definition includes those systems related to:

a. Intelligence activities

b. Cryptologic activities related to national security

c. Command and control of military forces

d. A weapon or weapon system

e. The direct fulfillment of military or intelligence missions, but not routine administrative or business applications.

12. Open Systems Environment (OSE). A computing environment designed to be interoperable and independent of hardware limitations. It consists of three main architectures: Communication Architecture, Information Processing Architecture and Data Administration Architecture.

13. Protocol Standards. Protocol standards delineate the sets of rules or conventions governing the exchange of information between computer systems, which also includes their peripheral devices. They can be either technical or procedural standards.

14. Router. A device or series of devices which delivers a s message to the destination node via intermediate nodes of one or more networks. A message may be required to pass through a series of intermediate nodes before it is finally delivered to the final destination. A key function of a router is determining the next node to which a message is sent.

15. Tactical Systems. Systems which support variable locations, i.e., mobile in support of FMF activities. These systems commonly operate in a stressed environment.